

What is claimed is:

1 1. An elliptic curve arithmetic operation device for
2 performing one of an addition and a doubling on an elliptic curve
3 $E: y^2=f(x)$ on a residue class ring of polynomials in two
4 variables α and β , moduli of the residue class ring being
5 polynomials $\beta^2-f(\alpha)$ and $h(\alpha)$, where $f(\alpha)=\alpha^3+a\alpha+b$, a and b are
6 constants, and $h(\alpha)$ is a polynomial in the variable α , the
7 elliptic curve arithmetic operation device comprising:

8 acquiring means for acquiring affine coordinates of at least
9 one point on the elliptic curve E and operation information
10 indicating one of the addition and the doubling, from an external
11 source;

12 transforming means for performing a coordinate transformation
13 on the acquired affine coordinates to generate Jacobian
14 coordinates, the coordinate transformation being transforming
15 affine coordinates $(\phi(\alpha), \beta \times \phi(\alpha))$ of a given point on the elliptic
16 curve E using polynomials

$$17 \qquad X(\alpha)=f(\alpha) \times \phi(\alpha)$$

$$18 \qquad Y(\alpha)=f(\alpha)^2 \times \phi(\alpha)$$

$$19 \qquad Z(\alpha)=1$$

20 into Jacobian coordinates $(X(\alpha):Y(\alpha):\beta \times Z(\alpha))$, $\phi(\alpha)$ and $\phi(\alpha)$
21 being polynomials; and

22 operating means for performing one of the addition and the
23 doubling indicated by the acquired operation information, on the

generated Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve E .

2. The elliptic curve arithmetic operation device of Claim 1,

wherein the acquiring means

(a) in a first case acquires affine coordinates of two different points on the elliptic curve E and operation information indicating the addition, and

(b) in a second case acquires affine coordinates of a single point on the elliptic curve E and operation information indicating the doubling,

wherein the transforming means

(a) in the first case performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates of the single point, and

wherein the operating means

(a) in the first case performs the addition indicated by the acquired operation information on the generated Jacobian coordinates of the two different points to obtain the Jacobian coordinates of the point on the elliptic curve E , and

(b) in the second case performs the doubling indicated by the acquired operation information on the generated Jacobian coordinates of the single point to obtain the Jacobian coordinates of the point on the elliptic curve E .

3. The elliptic curve arithmetic operation device of Claim 2,

wherein in the first case

the acquiring means acquires affine coordinates

$$(X1(\alpha), \beta \times Y1(\alpha))$$

$$(X2(\alpha), \beta \times Y2(\alpha))$$

of the two different points on the elliptic curve E and the operation information indicating the addition,

the transforming means performs the coordinate transformation on the acquired affine coordinates of the two different points to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta \times Z1(\alpha))$$

$$(X2(\alpha) : Y2(\alpha) : \beta \times Z2(\alpha))$$

of the two different points, and

the operating means computes

$$U1(\alpha) = X1(\alpha) \times Z2(\alpha)^2$$

$$U2(\alpha) = X2(\alpha) \times Z1(\alpha)^2$$

$$S1(\alpha) = Y1(\alpha) \times Z2(\alpha)^3$$

$$S2(\alpha) = Y2(\alpha) \times Z1(\alpha)^3$$

$$20 \quad H(\alpha) = U2(\alpha) - U1(\alpha)$$

$$21 \quad r(\alpha) = S2(\alpha) - S1(\alpha)$$

22 and computes

$$23 \quad X3(\alpha) = -H(\alpha)^3 - 2 \times U1(\alpha) \times H(\alpha)^2 + r(\alpha)^2$$

$$24 \quad Y3(\alpha) = -S1(\alpha) \times H(\alpha)^3 + r(\alpha) \times (U1(\alpha) \times H(\alpha)^2 - X3(\alpha))$$

$$25 \quad Z3(\alpha) = Z1(\alpha) \times Z2(\alpha) \times H(\alpha)$$

26 to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta \times Z3(\alpha))$ of the
27 point on the elliptic curve E .

1 4. The elliptic curve arithmetic operation device of Claim
2 2,

3 wherein in the second case

4 the acquiring means acquires affine coordinates

$$5 \quad (X1(\alpha), \beta \times Y1(\alpha))$$

6 of the single point on the elliptic curve E and the operation
7 information indicating the doubling,

8 the transforming means performs the coordinate transformation
9 on the acquired affine coordinates of the single point to
10 generate Jacobian coordinates

$$11 \quad (X1(\alpha) : Y1(\alpha) : \beta \times Z1(\alpha))$$

12 of the single point, and

13 the operating means computes

$$14 \quad S(\alpha) = 4 \times X1(\alpha) \times Y1(\alpha)^2$$

$$15 \quad M(\alpha) = 3 \times X1(\alpha)^2 + a \times Z1(\alpha)^4 \times f(\alpha)^2$$

16 $T(\alpha) = -2 \times S(\alpha) + M(\alpha)^2$
17 and computes
18 $X3(\alpha) = T(\alpha)$
19 $Y3(\alpha) = -8 \times Y1(\alpha)^4 + M(\alpha) \times (S(\alpha) - T(\alpha))$
20 $Z3(\alpha) = 2 \times Y1(\alpha) \times Z1(\alpha)$
21 to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta \times Z3(\alpha))$ of the
22 point on the elliptic curve E .

1 5. The elliptic curve arithmetic operation device of Claim
2 2,

3 wherein the acquiring means

4 (a) in the first case acquires affine coordinates

5 $(X1(\alpha), \beta \times Y1(\alpha))$

6 $(X2(\alpha), \beta \times Y2(\alpha))$

7 of the two different points on the elliptic curve E and the
8 operation information indicating the addition, and

9 (b) in the second case acquires affine coordinates

10 $(X1(\alpha), \beta \times Y1(\alpha))$

11 of the single point on the elliptic curve E and the operation
12 information indicating the doubling,

13 wherein the transforming means

14 (a) in the first case performs the coordinate transformation
15 on the acquired affine coordinates of the two different points to
16 generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta \times Z1(\alpha))$$

$$(X2(\alpha) : Y2(\alpha) : \beta \times Z2(\alpha))$$

of the two different points, and

(b) in the second case performs the coordinate transformation on the acquired affine coordinates of the single point to generate Jacobian coordinates

$$(X1(\alpha) : Y1(\alpha) : \beta \times Z1(\alpha))$$

of the single point, and

wherein the operating means

(a) in the first case computes

$$U1(\alpha) = X1(\alpha) \times Z2(\alpha)^2$$

$$U2(\alpha) = X2(\alpha) \times Z1(\alpha)^2$$

$$S1(\alpha) = Y1(\alpha) \times Z2(\alpha)^3$$

$$S2(\alpha) = Y2(\alpha) \times Z1(\alpha)^3$$

$$H(\alpha) = U2(\alpha) - U1(\alpha)$$

$$r(\alpha) = S2(\alpha) - S1(\alpha)$$

and computes

$$X3(\alpha) = -H(\alpha)^3 - 2 \times U1(\alpha) \times H(\alpha)^2 + r(\alpha)^2$$

$$Y3(\alpha) = -S1(\alpha) \times H(\alpha)^3 + r(\alpha) \times (U1(\alpha) \times H(\alpha)^2 - X3(\alpha))$$

$$Z3(\alpha) = Z1(\alpha) \times Z2(\alpha) \times H(\alpha)$$

to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta \times Z3(\alpha))$ of the point on the elliptic curve E , and

(b) in the second case computes

$$S(\alpha) = 4 \times X1(\alpha) \times Y1(\alpha)^2$$

$$41 \quad M(\alpha) = 3 \times X1(\alpha)^2 + a \times Z1(\alpha)^4 \times f(\alpha)^2$$

$$42 \quad T(\alpha) = -2 \times S(\alpha) + M(\alpha)^2$$

43 and computes

$$44 \quad X3(\alpha) = T(\alpha)$$

$$45 \quad Y3(\alpha) = -8 \times Y1(\alpha)^4 + M(\alpha) \times (S(\alpha) - T(\alpha))$$

$$46 \quad Z3(\alpha) = 2 \times Y1(\alpha) \times Z1(\alpha)$$

47 to obtain the Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta \times Z3(\alpha))$ of
48 the point on the elliptic curve E .

1 6. An elliptic curve order computation device for computing
2 an order of an elliptic curve according to a Schoof-Elkies-Atkin
3 algorithm, comprising the elliptic curve arithmetic operation
4 device of Claim 1.

1 7. The elliptic curve order computation device of Claim 6
2 comprising the elliptic curve arithmetic operation device of
3 Claim 2.

1 8. The elliptic curve order computation device of Claim 7
2 comprising the elliptic curve arithmetic operation device of
3 Claim 5.

1 9. An elliptic curve construction device for determining
2 parameters of an elliptic curve E which is defined over a finite

field $GF(p)$ and offers a high level of security, p being a prime,
the elliptic curve construction device comprising:

random number generating means for generating a random
number;

parameter generating means for selecting the parameters of
the elliptic curve E using the generated random number, in such
a manner that a probability of a discriminant of the elliptic
curve E having any square factor is lower than a predetermined
threshold value;

finitude judging means for judging whether the elliptic curve
 E defined by the selected parameters has any point whose order is
finite on a rational number field;

order computing means for computing an order m of the
elliptic curve E when the finitude judging means judges that the
elliptic curve E does not have any point whose order is finite on
the rational number field;

security judging means for judging whether a condition that
the computed order m is a prime not equal to the prime p is
satisfied;

repeat controlling means for controlling the random number
generating means, the parameter generating means, the finitude
judging means, the order computing means, and the security
judging means respectively to repeat random number generation,
parameter selection, finitude judgement, order computation, and

27 security judgement) until the condition is satisfied; and
28 parameter outputting means for outputting the selected
29 parameters when the condition is satisfied.

1 10. The elliptic curve construction device of Claim 9,
2 wherein the elliptic curve E is expressed as $y^2 = x^3 + ax + b$,
3 where parameters a and b are constants, and
4 wherein the parameter generating means selects -3 and the
5 random number respectively as the parameters a and b so that the
6 probability of the discriminant of the elliptic curve E having
7 any square factor is lower than the predetermined threshold
8 value.

1 11. The elliptic curve construction device of Claim 10,
2 wherein the finitude judging means, given two primes $p1$ and
3 $p2$ beforehand where $p1 \neq p2$, interprets the elliptic curve E as an
4 elliptic curve EQ on the rational number field, computes orders
5 $m1$ and $m2$ of respective elliptic curves $Ep1$ and $Ep2$ which are
6 produced by reducing the elliptic curve EQ modulo $p1$ and $p2$,
7 judges whether the orders $m1$ and $m2$ are relatively prime, and, if
8 the orders $m1$ and $m2$ are relatively prime, judges that the
9 elliptic curve E does not have any point whose order is finite on
10 the rational number field.

1 12. The elliptic curve construction device of Claim 11,
2 wherein the finitude judging means, given the primes $p1=5$ and
3 $p2=7$ beforehand, computes the orders $m1$ and $m2$ of the respective
4 elliptic curves $Ep1$ and $Ep2$ produced by reducing the elliptic
5 curve EQ modulo $p1=5$ and $p2=7$.

1 13. The elliptic curve construction device of Claim 11,
2 wherein the order computing means computes the order m of the
3 elliptic curve E according to a Schoof-Elkies-Atkin algorithm and
4 includes

5 elliptic curve arithmetic operating means for performing one
6 of an addition and a doubling on the elliptic curve $E: y^2=f(x)$
7 on a residue class ring of polynomials in variables α and β ,
8 moduli of the residue class ring being polynomials $\beta^2-f(\alpha)$ and
9 $h(\alpha)$, where $f(\alpha)=\alpha^3+a\alpha+b$ and $h(\alpha)$ is a polynomial in the
10 variable α ,

11 wherein the elliptic curve arithmetic operating means
12 includes the elliptic curve arithmetic operation device of Claim
13 1.

1 14. The elliptic curve construction device of Claim 13,
2 wherein the elliptic curve arithmetic operating means
3 includes the elliptic curve arithmetic operation device of Claim
4 2.

1 15. The elliptic curve construction device of Claim 14,
2 wherein the elliptic curve arithmetic operating means
3 includes the elliptic curve arithmetic operation device of Claim
4 5.

1 16. An elliptic curve application device that uses elliptic
2 curves, comprising
3 elliptic curve constructing means for determining parameters
4 of an elliptic curve E which is defined over a finite field $GF(p)$
5 and offers a high level of security, p being a prime,
6 wherein the elliptic curve constructing means includes the
7 elliptic curve construction device of Claim 9.

1 17. The elliptic curve application device of Claim 16,
2 wherein the elliptic curve constructing means includes the
3 elliptic curve construction device of Claim 10.

1 18. The elliptic curve application device of Claim 17,
2 wherein the elliptic curve constructing means includes the
3 elliptic curve construction device of Claim 11.

1 19. The elliptic curve application device of Claim 18,
2 wherein the elliptic curve constructing means includes the

3 elliptic curve construction device of Claim 12.

1 20. The elliptic curve application device of Claim 18,
2 wherein the elliptic curve constructing means includes the
3 elliptic curve construction device of Claim 13.

1 21. The elliptic curve application device of Claim 20,
2 wherein the elliptic curve constructing means includes the
3 elliptic curve construction device of Claim 14.

1 22. The elliptic curve application device of Claim 21,
2 wherein the elliptic curve constructing means includes the
3 elliptic curve construction device of Claim 15.

1 23. An elliptic curve arithmetic operation method used in an
2 elliptic curve arithmetic operation device equipped with an
3 acquiring means, a transforming means, and an operating means,
4 for performing one of an addition and a doubling on an elliptic
5 curve $E: y^2=f(x)$ on a residue class ring of polynomials in two
6 variables α and β , moduli of the residue class ring being
7 polynomials $\beta^2-f(\alpha)$ and $h(\alpha)$, where $f(\alpha)=\alpha^3+a\alpha+b$, a and b are
8 constants, and $h(\alpha)$ is a polynomial in the variable α , the
9 elliptic curve arithmetic operation method comprising:
10 an acquiring step performed by the acquiring means, for

acquiring affine coordinates of at least one point on the elliptic curve E and operation information indicating one of the addition and the doubling, from an external source;

a transforming step performed by the transforming means, for performing a coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates, the coordinate transformation being transforming affine coordinates $(\phi(\alpha), \beta \times \phi(\alpha))$ of a given point on the elliptic curve E using polynomials

$$X(\alpha) = f(\alpha) \times \phi(\alpha)$$

$$Y(\alpha) = f(\alpha) \wedge^2 \times \phi(\alpha)$$

$$Z(\alpha) = 1$$

into Jacobian coordinates $(X(\alpha) : Y(\alpha) : \beta \times Z(\alpha))$, $\phi(\alpha)$ and $\phi(\alpha)$ being polynomials; and

an operating step performed by the operating means, for performing one of the addition and the doubling indicated by the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve E .

24. An elliptic curve construction method used in an elliptic curve construction device equipped with random number generating means, parameter generating means, finitude judging means, order computing means, security judging means, repeat controlling means, and parameter outputting means, for determining parameters

6 of an elliptic curve E which is defined over a finite field $GF(p)$
7 and offers a high level of security, p being a prime; the
8 elliptic curve construction method comprising:

9 a random number generating step performed by the random
10 number generating means, for generating a random number;

11 a parameter generating step performed by the parameter
12 generating means, for selecting the parameters of the elliptic
13 curve E using the generated random number, in such a manner that
14 a probability of a discriminant of the elliptic curve E having
15 any square factor is lower than a predetermined threshold
16 value;

17 a finitude judging step performed by the finitude judging
18 means, for judging whether the elliptic curve E defined by the
19 selected parameters has any point whose order is finite on a
20 rational number field;

21 an order computing step performed by the order computing
22 means, for computing an order m of the elliptic curve E when the
23 finitude judging step judges that the elliptic curve E does not
24 have any point whose order is finite on the rational number
25 field;

26 a security judging step performed by the security judging
27 means, for judging whether a condition that the computed order m
28 is a prime not equal to the prime p is satisfied;

29 a repeat controlling step performed by the repeat controlling

means, for controlling the random number generating step, the parameter generating step, the finitude judging step, the order computing step, and the security judging step respectively to repeat random number generation, parameter selection, finitude judgement, order computation, and security judgement until the condition is satisfied; and

a parameter outputting step performed by the parameter outputting means, for outputting the selected parameters when the condition is satisfied.

25. A computer-readable storage medium storing an elliptic curve arithmetic operation program used in an elliptic curve arithmetic operation device equipped with acquiring means, transforming means, and operating means, for performing one of an addition and a doubling on an elliptic curve $E: y^2=f(x)$ on a residue class ring of polynomials in two variables α and β , moduli of the residue class ring being polynomials $\beta^2-f(\alpha)$ and $h(\alpha)$, where $f(\alpha)=\alpha^3+a\alpha+b$, a and b are constants, and $h(\alpha)$ is a polynomial in the variable α , the elliptic curve arithmetic operation program comprising:

an acquiring step performed by the acquiring means, for acquiring affine coordinates of at least one point on the elliptic curve E and operation information indicating one of the addition and the doubling, from an external source;

15 a transforming step performed by the transforming means, for
16 performing a coordinate transformation on the acquired affine
17 coordinates to generate Jacobian coordinates, the coordinate
18 transformation being transforming affine coordinates $(\phi(\alpha), \beta \times \phi(\alpha))$ of a given point on the elliptic curve E using polynomials

$$X(\alpha) = f(\alpha) \times \phi(\alpha)$$

$$Y(\alpha) = f(\alpha)^2 \times \phi(\alpha)$$

$$Z(\alpha) = 1$$

23 into Jacobian coordinates $(X(\alpha) : Y(\alpha) : \beta \times Z(\alpha))$, $\phi(\alpha)$ and $\phi(\alpha)$
24 being polynomials; and

25 an operating step performed by the operating means, for
26 performing one of the addition and the doubling indicated by the
27 acquired operation information, on the generated Jacobian
28 coordinates to obtain Jacobian coordinates of a point on the
29 elliptic curve E .

1 26. The storage medium of Claim 25,

2 wherein the acquiring step

3 (a) in a first case acquires affine coordinates of two
4 different points on the elliptic curve E and operation
5 information indicating the addition, and

6 (b) in a second case acquires affine coordinates of a single
7 point on the elliptic curve E and operation information
8 indicating the doubling,

9 wherein the transforming step

10 (a) in the first case performs the coordinate transformation
11 on the acquired affine coordinates of the two different points to
12 generate Jacobian coordinates of the two different points, and

13 (b) in the second case performs the coordinate transformation
14 on the acquired affine coordinates of the single point to
15 generate Jacobian coordinates of the single point, and

16 wherein the operating step

17 (a) in the first case performs the addition indicated by the
18 acquired operation information on the generated Jacobian
19 coordinates of the two different points to obtain the Jacobian
20 coordinates of the point on the elliptic curve E , and

21 (b) in the second case performs the doubling indicated by the
22 acquired operation information on the generated Jacobian
23 coordinates of the single point to obtain the Jacobian
24 coordinates of the point on the elliptic curve E .

1 27. The storage medium of Claim 26,

2 wherein in the first case

3 the acquiring step acquires affine coordinates

4 $(X1(\alpha), \beta \times Y1(\alpha))$

5 $(X2(\alpha), \beta \times Y2(\alpha))$

6 of the two different points on the elliptic curve E and the
7 operation information indicating the addition,

8 the transforming step performs the coordinate transformation
 9 on the acquired affine coordinates of the two different points to
 10 generate Jacobian coordinates

$$11 \qquad (X1(\alpha) : Y1(\alpha) : \beta \times Z1(\alpha))$$

$$12 \qquad (X2(\alpha) : Y2(\alpha) : \beta \times Z2(\alpha))$$

13 of the two different points, and
 14 the operating step computes

$$15 \qquad U1(\alpha) = X1(\alpha) \times Z2(\alpha)^2$$

$$16 \qquad U2(\alpha) = X2(\alpha) \times Z1(\alpha)^2$$

$$17 \qquad S1(\alpha) = Y1(\alpha) \times Z2(\alpha)^3$$

$$18 \qquad S2(\alpha) = Y2(\alpha) \times Z1(\alpha)^3$$

$$19 \qquad H(\alpha) = U2(\alpha) - U1(\alpha)$$

$$20 \qquad r(\alpha) = S2(\alpha) - S1(\alpha)$$

21 and computes

$$22 \qquad X3(\alpha) = -H(\alpha)^3 - 2 \times U1(\alpha) \times H(\alpha)^2 + r(\alpha)^2$$

$$23 \qquad Y3(\alpha) = -S1(\alpha) \times H(\alpha)^3 + r(\alpha) \times (U1(\alpha) \times H(\alpha)^2 - X3(\alpha))$$

$$24 \qquad Z3(\alpha) = Z1(\alpha) \times Z2(\alpha) \times H(\alpha)$$

25 to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta \times Z3(\alpha))$ of the
 26 point on the elliptic curve E .

1 28. The storage medium of Claim 26,
 2 wherein in the second case
 3 the acquiring step acquires affine coordinates

$$4 \qquad (X1(\alpha), \beta \times Y1(\alpha))$$

5 of the single point on the elliptic curve E and the operation
6 information indicating the doubling,

7 the transforming step performs the coordinate transformation
8 on the acquired affine coordinates of the single point to
9 generate Jacobian coordinates

$$10 \quad (X1(\alpha) : Y1(\alpha) : \beta \times Z1(\alpha))$$

11 of the single point, and

12 the operating step computes

$$13 \quad S(\alpha) = 4 \times X1(\alpha) \times Y1(\alpha)^2$$

$$14 \quad M(\alpha) = 3 \times X1(\alpha)^2 + a \times Z1(\alpha)^4 \times f(\alpha)^2$$

$$15 \quad T(\alpha) = -2 \times S(\alpha) + M(\alpha)^2$$

16 and computes

$$17 \quad X3(\alpha) = T(\alpha)$$

$$18 \quad Y3(\alpha) = -8 \times Y1(\alpha)^4 + M(\alpha) \times (S(\alpha) - T(\alpha))$$

$$19 \quad Z3(\alpha) = 2 \times Y1(\alpha) \times Z1(\alpha)$$

20 to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta \times Z3(\alpha))$ of the
21 point on the elliptic curve E .

1 29. The storage medium of Claim 26,

2 wherein the acquiring step

3 (a) in the first case acquires affine coordinates

$$4 \quad (X1(\alpha), \beta \times Y1(\alpha))$$

$$5 \quad (X2(\alpha), \beta \times Y2(\alpha))$$

6 of the two different points on the elliptic curve E and the

7 operation information indicating the addition, and
 8 (b) in the second case acquires affine coordinates
 9 $(X1(\alpha), \beta \times Y1(\alpha))$
 10 of the single point on the elliptic curve E and the operation
 11 information indicating the doubling,
 12 wherein the transforming step
 13 (a) in the first case performs the coordinate transformation
 14 on the acquired affine coordinates of the two different points to
 15 generate Jacobian coordinates
 16 $(X1(\alpha) : Y1(\alpha) : \beta \times Z1(\alpha))$
 17 $(X2(\alpha) : Y2(\alpha) : \beta \times Z2(\alpha))$
 18 of the two different points, and
 19 (b) in the second case performs the coordinate transformation
 20 on the acquired affine coordinates of the single point to
 21 generate Jacobian coordinates
 22 $(X1(\alpha) : Y1(\alpha) : \beta \times Z1(\alpha))$
 23 of the single point, and
 24 wherein the operating step
 25 (a) in the first case computes
 26 $U1(\alpha) = X1(\alpha) \times Z2(\alpha)^2$
 27 $U2(\alpha) = X2(\alpha) \times Z1(\alpha)^2$
 28 $S1(\alpha) = Y1(\alpha) \times Z2(\alpha)^3$
 29 $S2(\alpha) = Y2(\alpha) \times Z1(\alpha)^3$
 30 $H(\alpha) = U2(\alpha) - U1(\alpha)$

$$31 \quad r(\alpha) = S2(\alpha) - S1(\alpha)$$

32 and computes

$$33 \quad X3(\alpha) = -H(\alpha)^3 - 2 \times U1(\alpha) \times H(\alpha)^2 + r(\alpha)^2$$

$$34 \quad Y3(\alpha) = -S1(\alpha) \times H(\alpha)^3 + r(\alpha) \times (U1(\alpha) \times H(\alpha)^2 - X3(\alpha))$$

$$35 \quad Z3(\alpha) = Z1(\alpha) \times Z2(\alpha) \times H(\alpha)$$

36 to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta \times Z3(\alpha))$ of the
37 point on the elliptic curve E , and

38 (b) in the second case computes

$$39 \quad S(\alpha) = 4 \times X1(\alpha) \times Y1(\alpha)^2$$

$$40 \quad M(\alpha) = 3 \times X1(\alpha)^2 + a \times Z1(\alpha)^4 \times f(\alpha)^2$$

$$41 \quad T(\alpha) = -2 \times S(\alpha) + M(\alpha)^2$$

42 and computes

$$43 \quad X3(\alpha) = T(\alpha)$$

$$44 \quad Y3(\alpha) = -8 \times Y1(\alpha)^4 + M(\alpha) \times (S(\alpha) - T(\alpha))$$

$$45 \quad Z3(\alpha) = 2 \times Y1(\alpha) \times Z1(\alpha)$$

46 to obtain the Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta \times Z3(\alpha))$ of
47 the point on the elliptic curve E .

1 30. A computer-readable storage medium storing an elliptic
2 curve construction program used in an elliptic curve construction
3 device equipped with random number generating means, parameter
4 generating means, finitude judging means, order computing means,
5 security judging means, repeat controlling means, and parameter
6 outputting means, for determining parameters of an elliptic curve

7 E which is defined over a finite field $GF(p)$ and offers a high
8 level of security, p being a prime, the elliptic curve
9 construction program comprising:

10 a random number generating step performed by the random
11 number generating means, for generating a random number;

12 a parameter generating step performed by the parameter
13 generating means, for selecting the parameters of the elliptic
14 curve E using the generated random number, in such a manner that
15 a probability of a discriminant of the elliptic curve E having
16 any square factor is lower than a predetermined threshold
17 value;

18 a finitude judging step performed by the finitude judging
19 means, for judging whether the elliptic curve E defined by the
20 selected parameters has any point whose order is finite on a
21 rational number field;

22 an order computing step performed by the order computing
23 means, for computing an order m of the elliptic curve E when the
24 finitude judging step judges that the elliptic curve E does not
25 have any point whose order is finite on the rational number
26 field;

27 a security judging step performed by the security judging
28 means, for judging whether a condition that the computed order m
29 is a prime not equal to the prime p is satisfied;

30 a repeat controlling step performed by the repeat controlling

31 means, for controlling the random number generating step, the
32 parameter generating step, the finitude judging step, the order
33 computing step, and the security judging step respectively to
34 repeat random number generation, parameter selection, finitude
35 judgement, order computation, and security judgement until the
36 condition is satisfied; and

37 a parameter outputting step performed by the parameter
38 outputting means, for outputting the selected parameters when the
39 condition is satisfied.

1 31. The storage medium of Claim 30,
2 wherein the elliptic curve E is expressed as $y^2 = x^3 + ax + b$,
3 where parameters a and b are constants, and
4 wherein the parameter generating step selects -3 and the
5 random number respectively as the parameters a and b so that the
6 probability of the discriminant of the elliptic curve E having
7 any square factor is lower than the predetermined threshold
8 value. α

1 32. The storage medium of Claim 31,
2 wherein the finitude judging step, given two primes p_1 and
3 p_2 beforehand where $p_1 \neq p_2$, interprets the elliptic curve E as an
4 elliptic curve EQ on the rational number field, computes orders
5 m_1 and m_2 of respective elliptic curves Ep_1 and Ep_2 which are

6 produced by reducing the elliptic curve EQ modulo p_1 and p_2 ,
7 judges whether the orders m_1 and m_2 are relatively prime, and, if
8 the orders m_1 and m_2 are relatively prime, judges that the
9 elliptic curve E does not have any point whose order is finite on
10 the rational number field.

1 33. The storage medium of Claim 32,
2 wherein the finitude judging step, given the primes $p_1=5$ and
3 $p_2=7$ beforehand, computes the orders m_1 and m_2 of the respective
4 elliptic curves Ep_1 and Ep_2 produced by reducing the elliptic
5 curve EQ modulo $p_1=5$ and $p_2=7$.